



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/763,103	04/12/2001	Melih Abdulhayoglu	148/259	3494
23638	7590	08/04/2004	EXAMINER	
ADAM EVANS, P.A. (formerly Adams, Schwartz & Evans, P.A.) 2180 TWO WACHOVIA CENTER CHARLOTTE, NC 28282			SHERKAT, AREZOO	
			ART UNIT	PAPER NUMBER
			2131	

DATE MAILED: 08/04/2004

8

Please find below and/or attached an Office communication concerning this application or proceeding.

8

Office Action Summary	Application No.	Applicant(s)
	09/763,103	ABDULHAYOGLU, MELIH
	Examiner Arezoo Sherkat	Art Unit 2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 12 April 2001.

2a) This action is FINAL. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 26-50 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) Claim(s) _____ is/are allowed.

6) Claim(s) 26-50 is/are rejected.

7) Claim(s) _____ is/are objected to.

8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on 12 April 2001 is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a) All b) Some * c) None of:

1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)

2) Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 6.

4) Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.

5) Notice of Informal Patent Application (PTO-152)

6) Other: _____.

DETAILED ACTION

Claims 26-50 are presented for examination.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 26-50 are rejected under 35 U.S.C. 102(b) as being anticipated by Eldridge et al., (U.S. Patent No. 5,787,169 and Eldridge hereinafter).

Regarding claims 26 and 27, Eldridge discloses a method for password enhancing, which method comprises the steps of entering a user password and irreversibly encrypting the user password (i.e., calculating the hash value for the entered password)(Col. 4, lines 37-67).

Regarding claim 33, 34, and 35, Eldridge discloses comparing the enhanced password with a password associated with the data, and permitting access to the data only if the enhanced password and the data password correspond (Col. 6, lines 48-67 and Col. 7, lines 1-48).

Regarding claim 36 and 47, Eldridge discloses a data communication system comprising an input device for generating a plurality of input signals available from a set of input signals and a character generator configured to receive an input signal and generate an output signal comprising a plurality of signals from the set of input signals in which the output signal is different from the signal input to the character generator (Col. 5, lines 59-67 and Col. 6, lines 1-7).

Regarding claims 37 and 38, Eldridge discloses in which the output signal is of a different length to the signal input to the character generator (i.e., the combination of steps 302 and 306 in Fig. 3 produces an output which is different from/longer than the password 304)(Col. 5, lines 59-67 and Col. 6, lines 1-7).

Regarding claims 39 and 40, Eldridge discloses in which the comparison means further comprises means for outputting a signal dependent upon the correspondence of the output signal with the stored password (Col. 6, lines 48-67 and Col. 7, lines 1-67).

Regarding claims 41 and 42, Eldridge discloses in which the set of available input signals comprises all or part of the character set of the keyboard (Col. 3, lines 38-61).

Regarding claim 43, Eldridge discloses in which the system comprises a first input and a second input in which the character generator receives signals from the first

Art Unit: 2131

input and does not receive signals from the second input (i.e., password is entered through keyboard. The computer also includes a communications adapter which allows the system to be interconnected to a local area network or a wide area network)(Col. 3, lines 38-61).

Regarding claim 44, Eldridge discloses in which the first input is a local input device such as a keyboard or microphone and the second input is a remote based input device typically providing signals via a modem connection (i.e., password is entered through keyboard. The computer also includes a communications adapter which allows the system to be interconnected to a local area network or a wide area network)(Col. 3, lines 38-61).

Regarding claims 45 and 46, Eldridge discloses in which the set of input signals comprises alphanumeric characters (Col. 3, lines 38-61).

Regarding claim 48, Eldridge discloses a data communication method comprising receiving an input signal available from a set of input signals, generating an output signal comprising a plurality of signals from the set of available input signals, in which the output signal is different from the input signal (Col. 3, lines 62-67 and Col. 4-5, lines 1-67 and Col. 6, lines 1-47).

Regarding claim 49, Eldridge discloses in which the method further comprises the step of repeating the operation for a plurality of input signals (Col. 3, lines 62-67 and Col. 4-5, lines 1-67).

Regarding claim 50, Eldridge discloses in which the output signals vary in length one from the other (i.e., the input, password 304 is different each time therefore the output are different from each other)(Col. 5, lines 59-67 and Col. 6, lines 1-7).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 20-32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Eldridge et al., (U.S. Patent No. 5,787,169 and Eldridge hereinafter), in view of Dolan et al. (U.S. Patent No. 5,604,801 and Dolan hereinafter).

Regarding claim 28, Eldridge does not expressly disclose in which the method comprises the additional step of using an encrypted first stored key (NEPKEY) to encrypt the irreversibly encrypted user password (HASH).

However, Dolan discloses in which the method comprises the additional step of using an encrypted first stored key (NEPKEY) to encrypt the irreversibly encrypted user

password (HASH)(i.e., the signer encrypts the hash value of the message using private key)(Col. 1, lines 40-59).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Eldridge with the teachings of Dolan because it would allow to include the additional step of using an encrypted first stored key (NEPKEY) to encrypt the irreversibly encrypted user password (HASH) with the motivation to provide a communications system in which messages are processed using public key cryptography with a private key unique to one or more users under the control of a portable security device (Dolan, Col. 2, lines 65-67 and Col. 3, lines 1-5).

Regarding claim 29, Eldridge does not expressly disclose in which the first stored key is encrypted by a public key encryption algorithm.

However, Dolan discloses in which the first stored key is encrypted by a public key encryption algorithm (Col. 10, lines 20-45).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Eldridge with the teachings of Dolan because it would allow to include in which the first stored key is encrypted by a public key encryption algorithm with the motivation to provide a communications system in which messages are processed using public key cryptography with a private key unique to one or more users under the control of a portable security device (Dolan, Col. 2, lines 65-67 and Col. 3, lines 1-5).

Regarding claim 30, Eldridge does not expressly disclose in which the method comprises the additional step of decrypting an encrypted second stored key (UPEK) using the decrypted first stored key (NEPKEY).

However, Dolan discloses in which the method comprises the additional step of decrypting an encrypted second stored key (UPEK) using the decrypted first stored key (NEPKEY)(Col. 8, lines 39-67 and Col. 9, lines 1-67 and Col. 10, lines 1-15).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Eldridge with the teachings of Dolan because it would allow to include the additional step of decrypting an encrypted second stored key (UPEK) using the decrypted first stored key (NEPKEY) with the motivation to provide a communications system in which messages are processed using public key cryptography with a private key unique to one or more users under the control of a portable security device (Dolan, Col. 2, lines 65-67 and Col. 3, lines 1-5).

Regarding claim 31, Eldridge does not expressly disclose in which the second stored key is encrypted by a reversible algorithm.

However, Dolan discloses in which the second stored key is encrypted by a reversible algorithm (Col. 10, lines 20-45).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Eldridge with the teachings of Dolan because it would allow to include in which the second stored key is encrypted by a reversible algorithm with the motivation to provide a communications system in which

messages are processed using public key cryptography with a private key unique to one or more users under the control of a portable security device (Dolan, Col. 2, lines 65-67 and Col. 3, lines 1-5).

Regarding claim 32, Eldridge does not expressly disclose in which the result (HASH) of the irreversibly encrypted user password is encrypted using the second stored key (UPEK) as an encryption key.

However, Dolan discloses in which the result (HASH) of the irreversibly encrypted user password is encrypted using the second stored key (UPEK) as an encryption key (Col. 8, lines 39-67 and Col. 9, lines 1-67 and Col. 10, lines 1-15).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify the teachings of Eldridge with the teachings of Dolan because it would allow to include in which the result (HASH) of the irreversibly encrypted user password is encrypted using the second stored key (UPEK) as an encryption key with the motivation to provide a communications system in which messages are processed using public key cryptography with a private key unique to one or more users under the control of a portable security device (Dolan, Col. 2, lines 65-67 and Col. 3, lines 1-5).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Angelo et al., (U.S. Patent No. 5,953,422),

Matyas et al., (U.S. Patent No. 4,924,515),
Grawrock et al., (U.S. Patent No. 6,339,828),
Kaufman, (U.S. Patent No. 6,178,508),
Kaufman, (U.S. Patent No. 5,666,415), and
Davis et al., (U.S. Patent No. 6,064,736).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Arezoo Sherkat whose telephone number is (703) 305-8749. The examiner can normally be reached on 8:00-4:30 Monday-Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

A. Sherkat
Arezoo Sherkat
Patent Examiner
Group 2131
July 26, 2004

Ayaz Sheikh
AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100